

**8th ANNUAL SUMMIT
CHIEF INFORMATION SECURITY OFFICER
MIDDLE EAST
Dubai 29th February – 4th March, 2016**

‘A CISO’S PLACE ISON THE MAIN BOARD!’

**Lady Olga Maitland
Chairman
Copenhagen Compliance® UK Ltd.**

Agenda

- Can a company Board afford not to have you?
- New Board trends
 - Unprecedented' demand for CIOs/CISOs to serve as a director on the board.
- The spur: Global cost of cyber attacks

Exorbitant costs

- The price to pay
 - \$575b lost globally at a cost of 90m attacks¹.
- The crisis after a major cyber attack.
- The fact is criminals & pranksters are thriving

¹ **Source;** Waratek (named top Innovator in Data Protection 2015)

A moving role and target

- Cyber attacks are not just an IT or technical issue, it's a business issue.
- Increasing the size and budget of security teams.
- A CISO has to be proactive in persuading his Board to invest in cyber security

CISO'S role is changing

- CISO'S NEW RESPONSIBILITIES
- Increasing pressure from stakeholders to provide reassurance that cyber risks are actively managed.
- Cyber threats are estimated to cost the UK economy billions of pounds
 - with a near doubling of attacks last year alone

Outlook for 2016

- New Threats
- Responding to threats
- Cyber-crime will spread into all sectors, bringing more companies into the firing line.
- Sectors most engaged with cyber security are telecommunications, and financial services
 - especially where personal data is involved
 - Many serious gaps do come to light.

Middle East cyber targets

- Saudi Arabia suffered cyber attack on Aramco in 2012
 - damaged 30,000 of the firms computers
 - Ministry of Petroleum & Mineral Resources & Saudi Airlines are making their own investment
- Qatar is investing in a comprehensive cyber security infrastructure
 - in preparation for the FIFA World Cup in 2022.
- Bahrain has been examining its own ability to withstand a cyber attack
- Abu Dhabi established the National Electronic Security Authority –
- UAE suffered from attacks on their oil, gas & helium industries
- The Petroleum Oil Company in Kuwait will spend \$1b on cyber security.
- Shortage of highly skilled software engineers in IT security

New Threats in the Middle East

- ‘Cutting Sword of Justice’ responsible
- A group ‘Desert Falcons’ has emerged
- New threats from Iran, are increasing rapidly
- The ingenuity of the Daesh is determined
- A dedicated IT security budget - must grow.
- Cyber security as a business enabler.
- Investment to enhance protection

Responding to the threats

- The CISO is too far down the chain to be heard.
- Companies have been ill equipped to defend.
- Under pressure from stakeholders to provide assurance
- Lack of cyber awareness at board level
- Restricted budgets, and only grudgingly given.
- Drain on budgets. No evidence of profit
- Until a major cyber-attack and the costs are open

How should a CISO present & persuade?

- Think business
- Take advantage of any major cyber attack R relate the risks
- Media coverage with public outrage a sharp awakener.
- The principles are clear and without jargon.
 - A short succinct paper circulated in advance helps
- Responsibility is oversight and governance.
- The case for investment has been poorly explained;

CISO is a businessman & a technician

- The soft language of business & communication, free of jargon
- Establish trust and credibility with tech-savvy directors
- The solution is on money and not a technical solution
- Training when staff become a hackers tool
- Talk up systems which need attention and enhance protection
- Use analogies to explain technical concepts in layman's terms
- Align the security risks alongside the business goals
- The business aspect of strategy, prioritisation and control
- Answer the standard Board room question: 'how secure are we?'
- Socialise the message, so that this is a team story

The really hard work begins...

- Redefine the CISO aspiration in the organisation
- Improve technology equipment and data products
- Streamline the key processes & support functions
 - Reinvent business models & IT/data driven services
- Develop a digital services & technology platform
- With a secure cloud, big data and analytics
- Digital governance includes ; governance, culture and processes

CONCLUSION

- Expect changes on the CISO, role, function and responsibility throughout the organisation
- Rather like a rider on top of an elephant with a small stick –
 - not in a position of authority, but in a position of influence.
- See information risk as a key aspect for stability & profitability
- Cyber risk is now considered one of the top three business risks.
- Senior executives care about information risk management
 - They need to hear the full story directly from the security leader

THANK YOU!

**Lady Olga Maitland
Chairman**

Copenhagen Compliance[®] UK Ltd

Email: olga.maitland@virgin.net

Mobile : +44 7778 917133